Interview Summary

1.   A proposed amendment was submitted for applicant's consideration. Examiner

suggested Applicant to amend claims as shown in the Examiner's Amendment below in

order to place the application in condition for allowance.

Examiner's Amendment

2.   An examiner's amendment to the record appears below. Should the changes

and/or additions be unacceptable to applicant, an amendment may be filed as provided

by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be

submitted no later than the payment of the issue fee.

3.   Authorization for this examiner's amendment was given in a telephone interview

with the Applicant's Representative, Cindy S. Kaplan (Reg. No. 40,043), on 13 May

2008.

IN THE SPECIFICATION

Please replace the paragraph starting on page 17, line 10 as below:

FIG. 1 depicts a network device 100 that may be used to implement any of

the nodes depicted in FIGS. 2-3 or a network management workstation. In one

embodiment, network device 100 is a programmable machine that may be

implemented in hardware, software or any combination thereof. A processor 102

executes code stored in a program memory 104. Program memory 104 is one

example of a computer-readable storage medium. Program memory 104 can be a

volatile memory. Another form of computer-readable storage medium storing the

same codes would be some type of non-volatile storage such as floppy disks, CD-

ROMs, DVD-ROMs, hard disks, flash memory, etc. A carrier wave that carries the

code across a network is another example of a computer-readable storage medium.

IN THE CLAIMS

Please replace all claims as shown below:

Claim 1 (currently amended): In a data communication network, a method for

protecting a node, said method comprising processes of:

identifying said node to be protected;

allocating a primary bandwidth pool on links of said data communication network

for use by primary paths;

allocating a backup bandwidth pool on said links of said data communication

network for use as a backup, said backup bandwidth pool on each of said links

comprising a bandwidth equal to at least a link speed minus a maximum reservable

bandwidth for said primary paths on said link;

identifying a link pair traversing said node to be protected, said link pair having a

bandwidth to be protected;

establishing as a backup for said link pair a set of one or more backup paths that

do not include said node and wherein said one or more backup paths collectively have

backup bandwidth greater than or equal to said bandwidth to be protected;

deducting, for each link included in said set of paths, from backup bandwidth

available for protecting said node, while not deducting from backup bandwidth available

for protecting other nodes in said data communication network; and

repeating said processes of identifying, establishing, and deducting for a plurality

of link pairs traversing said node without exceeding available backup bandwidth of links

used in establishing said backups;

wherein said bandwidth to be protected of said link pair comprises a lesser of

primary bandwidths of links of said link pair traversing said node to be protected.

Claims 2-3 (canceled).

Claim 4 (original): The method of claim 1 wherein said set of one or more paths

comprises one or more label switched paths.

Claim 5 (original): The method of claim 1 wherein said processes of identifying

and establishing occur under control of said node.

Claim 6 (original): The method of claim 1 wherein said processes of identifying

and establishing occur under control of a computer independent of said node.

Claim 7 (original): The method of claim 1 further comprising:

signaling said backups to other nodes adjacent to said node in said data

communication network.

Claim 8 (currently amended): A method for operating a data communication

network to provide protection to nodes in said data communication network, said

method comprising:

maintaining, for each of a plurality of links in said data communication network, a

primary bandwidth pool for use by primary paths and a backup bandwidth pool for use

by backup tunnels; and

establishing said backup tunnels to protect a plurality of nodes of said network,

each of said backup tunnels consuming backup bandwidth from backup bandwidth

pools of selected ones of said plurality of links; and

wherein all backup tunnels protecting any particular node of said network do not

consume more bandwidth on any link than provided by the link's backup bandwidth pool

but wherein there is at least one set of backup tunnels that protect disparate nodes and

that consume more bandwidth on at least one link than provided by said at least one

link's backup bandwidth pool, and

wherein establishing backup tunnels comprises signaling said backup tunnels

with zero bandwidth to adjacent nodes of each protected node <u>and performing backup</u>

<u>tunnel selection computations at each protected node for that protected node.</u>

Claim 9 (original): The method of claim 8 wherein at least one of said backup tunnels comprises a label switched path.

Claims 10-15 (canceled).

Claim 16 (currently amended): In a data communication network, a computer-readable storage medium encoded with a computer program ~~product~~ for protecting a node, said computer program ~~product~~ comprising:

code that identifies said node to be protected;

code that allocates a primary bandwidth pool on links of said data communication network for use by primary paths;

code that allocates a backup bandwidth pool on said links of said data communication network ~~for use as a backup~~, said backup bandwidth pool on each of said links ~~comprising a bandwidth~~ equal to at least a link speed minus a maximum reservable bandwidth for said primary paths on said link;

code that identifies a link pair traversing said node to be protected, said link pair having a bandwidth to be protected;

code that establishes a backup for said link pair a set of one or more backup paths that do not include said node and wherein one or more backup paths collectively have backup bandwidth greater than or equal to said bandwidth to be protected;

code that deducts, for each link included in said set of paths, from backup

bandwidth available for protecting said node, while not deducting from backup

bandwidth available for protecting other nodes in said data communication network; and

code that repeatedly invokes said code that identifies, establishes, and deducts

for a plurality of link pairs connected to said node without exceeding available backup

bandwidth of links used in establishing said backups; ~~and~~

~~a computer-readable storage medium that stores the codes;~~

wherein said bandwidth to be protected of said link pair comprises a lesser of

primary bandwidths of links of said link pair traversing said node to be protected.

Claims 17-18 (canceled).

Claim 19 (currently amended): The computer-readable storage medium ~~program~~

~~product~~ of claim 16 wherein said set of one or more paths comprises one or more label

switched paths.

Claim 20 (currently amended): The computer-readable storage medium ~~program~~

~~product~~ of claim 16 further comprising:

code that signals said backups to other nodes adjacent to said node in said data

communication network.

Claim 21 (currently amended): A computer-<u>readable storage medium encoded</u>

<u>with a computer</u> program ~~product~~ for operating a data communication network to

provide protection to nodes in the data communication network, said computer program

~~product~~ comprising:

code that maintains, for each of a plurality of links in said data communication

network a primary bandwidth pool for use by primary paths and a backup bandwidth

pool for use by backup tunnels; and

code that establishes said backup tunnels to protect a plurality of nodes of said

network, each of said backup tunnels reserving backup bandwidth from backup

bandwidth pools of selected ones of said plurality of links;

wherein all backup tunnels protecting any particular node of said network do not

consume more bandwidth on any link than provided by the link's backup bandwidth pool

but wherein there is at least one set of backup tunnels that protect disparate nodes and

that consume more bandwidth on at least one link than provided by said at least one

link's backup bandwidth pool; and

wherein code that establishes backup tunnels comprises code that signals said

backup tunnels with zero bandwidth to adjacent nodes of each protected node <u>and code</u>

<u>that performs backup tunnel selection computations at each protected node for that</u>

<u>protected node</u>

; ~~and~~

~~a computer-readable storage medium that stores the codes~~.

Claim 22 (currently amended): The computer-<u>readable storage medium</u> ~~program~~ ~~product~~ of claim 21 where at least one of said backup tunnels comprises a label switched path.

Claims 23-24 (canceled).

Claim 25 (currently amended): A network device for implementing a node in a data communication network, said network device comprising:

a processor; and

a memory storing instruction for said processor, said instructions comprising:

code that identifies said node to be protected;

code that allocates a primary bandwidth pool on links of said data communication network for use by primary paths;

code that allocates a backup bandwidth pool on said links of said data communication network ~~for use as a backup~~, said backup bandwidth pool on each of said links ~~comprising a bandwidth~~ equal to at least a link speed minus a maximum reservable bandwidth for said primary paths on said link;

code that identifies a link pair traversing said node to be protected, said link pair having a bandwidth to be protected;

code that establishes a backup for said link pair a set of one or more backup paths that do not include said node and wherein one or more backup paths collectively have backup bandwidth greater than or equal to said bandwidth to be protected;

code that deducts, for each link included in said set of paths, from backup bandwidth available for protecting said node, while not deducting from backup bandwidth available for protecting other nodes in said data communication network; and

code that repeatedly invokes said code that identifies, establishes, and deducts for a plurality of link pairs connected to said node without exceeding available backup bandwidth of links used in establishing said backups;

wherein said bandwidth to be protected of said link pair comprises a lesser of primary bandwidths of links of said link pair traversing said node to be protected.

Claims 26-27 (canceled).

Claim 28 (original): The network device of claim 25 wherein said set of one or more paths comprises one or more label switched paths.

Claim 29 (original): The network device of claim 25 wherein said instructions further comprise:

code that signals said backups to other nodes adjacent to said node in said data communication network.

Claim 30 (currently amended): A network device for implementing a node in a communication network, said network device comprising:

a processor; and

a memory storing instruction for said processor, said instructions comprising:

code that maintains, for each of a plurality of links in said data communication

network a primary bandwidth pool for use by primary paths and a backup bandwidth

pool for use by backup tunnels; and

code that establishes said backup tunnels to protect a plurality of nodes of said

network, each of said backup tunnels reserving backup bandwidth from backup

bandwidth pools of selected ones of said plurality of links;

wherein all backup tunnels protecting any particular node of said network do not

consume more bandwidth on any link than provided by the link's backup bandwidth pool

but wherein there is at least one set of backup tunnels that protect disparate nodes and

that consume more bandwidth on at least one link than provided by said at least one

link's backup bandwidth pool;

wherein code that establishes backup tunnels comprises code that signals said

backup tunnels with zero bandwidth to adjacent nodes of each protected node <u>and code</u>

<u>that performs backup tunnel selection computations at each protected node for that</u>

<u>protected node.</u>

Claim 31 (currently amended): The network device of claim 30 ~~where~~ <u>wherein</u> at

least one of said backup tunnels comprises a label switched path.

Claims 32-36 (canceled).

Claim 37 (previously presented): The method of claim 1 wherein establishing a set of one or more backup paths comprises performing backup path selection computations at said node to be protected.

Claim 38 (previously presented): The method of claim 1 further comprising dynamically adjusting said established backup paths in response to a change in one or more of said primary paths.

Claim 39 (previously presented): The method of claim 1 wherein said backup paths are established at said node to be protected.

Claim 40 (previously presented): The method of claim 1 further comprising signaling said one or more backup paths with zero bandwidth to one or more other nodes.

Claim 41 (previously presented): The method of claim 8 further comprising identifying a failure at said node to be protected and rerouting traffic, wherein said traffic is rerouted in less than 50 milliseconds.

Claim 42 (previously presented): The method of claim 8 wherein said primary bandwidth pool comprises a maximum amount of bandwidth that is available for allocation to primary paths.

Claim 43 (previously presented): The method of claim 8 wherein said backup

bandwidth pool comprises a maximum amount of bandwidth allocated for backup traffic.

Allowable Subject Matter

4.   Claims 1, 4-9, 16, 19-22, 25, 28-31, and 37-43 are allowed. The following is an

examiner's statement of reasons for allowance: In interpreting the claims, in light of the

specification and the authorized Examiner's Amendment on 13 May 2008, the Examiner

finds the claimed invention to be patentably distinct from the prior art of record.

5.   In regards to statutory subject matter, the Examiner interprets the claim language

of "a node" to be hardware as pointed out in page 17, lines 10-19 of applicant's

specification which state, "A processor 102 executes code stored in a program memory

104." And the claim language of "a computer-readable storage medium" to be hardware

as well as recited in page 17, lines 10-19 which state, "Another form of computer-

readable storage medium storing the same codes would be some type of non-volatile

storage such as floppy disks, CD-ROMs, DVD-ROMs, hard disks, flash memory, etc."

6.   **Kinoshita et al. (2002/0172149)** teaches when setting up a working path, a

protection path is automatically set up by taking each node on the working path as a

start point. A working path setup request message carrying "protection needed/not-

needed" information is transmitted from an ingress node toward an egress node along

the route of the working path. When transferring a path setup response message as a

response to it, each node autonomously determines the route of the protection path and sends out a protection path setup request message along the route of the protection path **(Kinoshita, abstract, figure 6, and corresponding text).**

7.   **Jain (2002/0112072)** teaches a system and method for the fast re-routing of data in a data communication network. A protection label path is formed between a base node and an end node wherein the protection path avoids an intermediate node between the base node and the end node. Availability of protection provided by the protection path is advertised within the network. A protected path is formed for communicating data, the protected path passing through the intermediate node. When a fault is detected in the network, the fault is avoided by using the protection path for communicating data. Thus, alternate paths are defined for bypassing entire network nodes. As such, the protection paths allow data to be re-routed so as to avoid failed network nodes as well as failed network links **(Jain, abstract, figure 1, and corresponding text).**

8.   **Shabtay et al. (6,895,441)** teaches a path reroute mechanism for use in communication networks comprising multiple searches for a routing path to restore traffic following a failure that could not be protected by a previously established protection route (i.e. protection tunnel, bypass, etc.) or for routing or rerouting of traffic paths for optimization or any other purpose. Each node advertises TLVs that include bandwidth allocation information used to derive the actual amount of bandwidth available for protection purposes, protected paths and unprotected paths or a portion of this information such as in the case where unprotected paths are not supported.

Searches are performed on larger and larger portions of the available bandwidth until a route for the path is found **(Shabtay, abstract, figure 8, and corresponding text).**

9.   **Anderson et al. (2002/0004843)** teaches a system, device, and method for bypassing network changes in a communication network pre-computes recovery paths to protect various primary paths. A fast detection mechanism is preferably used to detect network changes quickly, and communications are switched over from the primary paths to the recovery paths in order to bypass network changes. Forwarding tables are preferably frozen as new primary paths are computed, and communications are switched over from the recovery paths to the new primary paths in a coordinated manner in order to avoid temporary loops and invalid routes. New recovery paths are computed to protect the new primary paths **(Anderson, abstract, figure 1, and corresponding text).**

10.   However, the prior art of record fail to teach or suggest individually or in combination the claimed limitations of independent claims 1, 16 and 25, <u>wherein said bandwidth to be protected of said link pair comprises a lesser of primary bandwidths of links of said link pair traversing said node to be protected,</u> correlating to page 13, lines 4-11of the applicant's specification which state, "In one embodiment, a node is protected by providing backup tunnels for each pair of links traversing the node such that the total bandwidth of the backup tunnels exceeds the primary bandwidth of the link pair, i.e., the lesser of the primary bandwidths of the two links." See also page 14, line 21-page 15, line 9. Furthermore, the prior art of record fail to teach or suggest individually or in combination the claimed limitations of independent claims 8, 21, and

30, <u>wherein code that establishes backup tunnels comprises code that signals said</u>

<u>backup tunnels with zero bandwidth to adjacent nodes of each protected node,</u>

correlating to page 16, lines 14-21 of the applicant's specification which state, "The

backup tunnels are preferably signaled using, e.g., the RSVP protocol, although it is

possible to employ other protocols such as, e.g., label distribution protocol (LDP) as

known in the art. According to one embodiment of the present invention, there is no

signaling of backup bandwidth reservation for the backup tunnels--that is the backup

tunnels are signaled with zero bandwidth." See also page 14, line 21-page 15, line 9.

11.   These limitations, in conjunction with the other limitations in the independent

claims 1, 8, 16, 21, 25, and 30 are not specifically disclosed or remotely suggested in

the prior art of record. Therefore, claims 1, 4-9, 16, 19-22, 25, 28-31, and 37-43 are

allowed.

12.   Any comments considered necessary by applicant must be submitted no later

than the payment of the issue fee and, to avoid processing delays, should preferably

accompany the issue fee. Such submissions should be clearly labeled "Comments on

Statement of Reasons for Allowance."

        Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Ranodhi Serrao whose telephone number is (571) 272-

7967. The examiner can normally be reached on 8:00-4:30pm, M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Rupal Dharia can be reached on (571) 272-3880. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/R. N. S./

Examiner, Art Unit 2141

5/16/2008

/William C. Vaughn, Jr./

Supervisory Patent Examiner, Art Unit 2144